Estrategias de ciberseguridad que sirven para optimizar el teletrabajo en las empresas del municipio de Manaure en el departamento de la Guajira.

Yalesxi Magdaniel Pushaina

Director (a): Yesnir Redondo

Monografía como opción de grado para optar el título de ingeniería de sistemas

Universidad nacional abierta y a distancia UNAD

Escuela de ciencias básicas, tecnología e ingeniería -ECBTI

Ingeniería de Sistemas

2025

Resumen

La vulnerabilidad en la ciberseguridad de las empresas ubicadas en el municipio de Manaure en el departamento de la guajira, representa un desafío para la implementación segura del teletrabajo, especialmente en un contexto con limitada infraestructura tecnológica y baja alfabetización digital. Por esta razón, la siguiente monografía tiene como objetivo general revisar las estrategias de ciber seguridad, que optimizan el teletrabajo en las empresas de Manaure, a través de una metodología basada en una revisión documental sistemática con enfoque cualitativo, guiada por un protocolo que permitió la selección y análisis de 25 documentos relevantes, en donde se incluyeron artículos científicos, normas internacionales, informes, técnicos, leyes y tesis especializadas. Los resultados de esta revisión, evidenciaron que, aunque existen marcos normativos sólidos, la aplicación de los mismos dentro del contexto local, enfrenta barreras por limitaciones tecnológicas y por el capital humano; asimismo, se identificaron debilidades en la cultura organizacional y en la capacitación digital del personal, lo que aún incrementa la probabilidad de riesgos cibernéticos. Por lo que se concluyó que la mejora de la tecnología, la capacitación continua y la adaptación de normas a la realidad local son esenciales para brindar un fortalecimiento a la seguridad digital y a la eficiencia operativa, dando como recomendación, avanzar en estudios futuros que profundicen las limitaciones tecnológicas y culturales y en el diseño de estrategias innovadoras, culturalmente, atadas para dar garantía a la sostenibilidad y eficiencia del teletrabajo en el contexto.

Palabras clave: Estrategias, ciberseguridad, optimizar, teletrabajo, Manaure.

Abstract

The cybersecurity vulnerability of companies located in the municipality of Manaure, department of La Guajira, represents a challenge for the secure implementation of teleworking, especially in a context with limited technological infrastructure and low digital literacy. For this reason, this monograph seeks to review the cybersecurity strategies that optimize teleworking in companies in Manaure, using a methodology based on a systematic review of documents with a qualitative approach, guided by a protocol that allowed the selection and analysis of 25 relevant documents, including scientific articles, international standards, technical reports, laws, and specialized theses. The results of this review showed that, although solid regulatory frameworks exist, their application in the local context faces barriers due to technological and human capital limitations. Furthermore, weaknesses in organizational culture and staff digital training were identified, further increasing the likelihood of cyber risks. Therefore, it was concluded that technological improvement, continuous training, and the adaptation of standards to local realities are essential to strengthen digital security and operational efficiency. Future studies are recommended to delve deeper into the technological and cultural limitations, as well as to design innovative and culturally integrated strategies that ensure the sustainability and efficiency of teleworking in this context.

Keywords: Strategies, cybersecurity, optimization, teleworking, Manaure.

Tabla de contenido

Lista de tablas

Lista de apéndices

Introducción

En los últimos años, el desarrollo acelerado de las tecnologías digitales ha transformado profundamente las dinámicas laborales a nivel global (Torrealba, 2024). Uno de los cambios más significativos ha sido la adopción del teletrabajo con modalidad creciente en niveles sectores productivos, impulsado inicialmente por la emergencia sanitaria por COVID-19 y consolidada, posteriormente como una opción estratégica para dar garantía a la continuidad, operativa, flexibilidad, laboral y reducción de costos.

En este nuevo entorno digitalizado, las organizaciones enfrentan oportunidades y también desafíos sustanciales, en términos de seguridad de la información y protección de activos digitales (Cano & Monsalve, 2023).

En este contexto, la ciber seguridad se encuentra posicionada como un componente crítico en la gestión organizacional moderna, específicamente en escenario donde los límites entre lo personal y lo corporativo se diluyen a través de conexiones remota, dispositivos personales y redes de comunicación descentralizadas.

Las amenazas cibernéticas, parten desde el robo de información, confidencial, hasta ataques de ransonware o suplantación de la identidad, se han intensificados, afectándose, sólo grandes corporaciones, sino también pequeñas y medianas empresas que carecen de infraestructura robusta para hacerles frente. (Guaña et al., 2022)

Esta situación se agrava aún más en regiones con limitaciones estructurales, como con actividad precaria, es escasa alfabetización digital o ausencia de políticas públicas eficaces entre ellas muchas localidades de la región caribe colombiana.

En este contexto específico, el municipio de Mauren, en el departamento de la Guajira, caracterizado por su alta vulnerabilidad social, dependencia de sectores económicos, informales y acceso limitado a tecnologías emergentes, representa un caso de estudio relevante para garantizar cómo se articulan, o cómo no se articulan las estrategias de ciberseguridad en empresas locales, que adoptan el teletrabajo como medida transitorio o permanente.

Esta problemática no sólo es técnica, pues también tiene un aporte organizacional, educativo y cultural que exige una comprensión integral de factores que condicionan la implementación de buenas prácticas de seguridad informática en estos contextos. Desde una perspectiva académica, este estudio aporta análisis de las condiciones estructurales y operativas, que influyen en la adopción política de civil, seguridad, adaptada al teletrabajo, particularmente en zonas tradicionalmente marginadas del debate tecnológico.

En términos sociales, se trata de visibilidad las brechas digitales que podrían profundizar la desigualdad, si no se acompañan de estrategias de fortalecimiento institucional de este mismo modo, la óptica empresarial, el abordaje permite la identificación de oportunidades para la mejora la resiliencia de las organizaciones frente a riesgos digitales crecientes, a través de recomendaciones, prácticas y contextualizadas.

La presente monografía se inscribe en el paradigma interpretativo, priorizando la comprensión de la realidad, desde las particularidades locales y los marcos referenciales de actores implicados, a través de la aplicación de una revisión sistemática de literatura, como método principal, lo que permitió la identificación y organización de evidencia empírica, marcos normativos, experiencias, documentadas y propuesta replicable en entornos similares.

En este mismo sentido, el enfoque metodológico estuvo orientado por criterios de inclusión, rigurosos, análisis temático de los contenidos y validación a través de contraste con fuentes expertas y reconocidas.

Finalmente, el documento se encuentra estructurado de la siguiente manera, en primer lugar, se presenta la introducción descripción del problema con su respectiva, pregunta problematizada, justificación, objetivos.

Seguidamente se encuentra el marco de referencia conformado por el estado del arte, el marco teórico y el marco conceptual, luego se detalla el diseño metodológico, adoptado, especificando fuentes, criterios y procedimientos utilizados en la recolección, y posteriormente se exponen los resultados de la revisión organizados según las categorías emergentes. Finalmente se formulan conclusiones y recomendaciones junto con una reflexión sobre las posibles futuras líneas de investigación que emergen del estudio.

Descripción de problema

La pandemia de COVID-19 provocó un cambio radical en la forma en que las empresas operan, impulsando a muchas organizaciones a adoptar el teletrabajo como una medida necesaria para garantizar la continuidad de sus operaciones (Lazos et al., 2024).

De lo anterior, las empresas del municipio de Manaure en el departamento de la Guajira, no han sido una excepción y han implementado el teletrabajo como parte de su estrategia de adaptación, son embargo, esta transición trajo consigo desafíos significativos, especialmente en lo que respecta a la ciberseguridad.

En este sentido, la implementación del teletrabajo ha expuesto a las empresas del sector, a diversas vulnerabilidades cibernéticas, como la falta de medidas adecuadas de ciberseguridad, lo cual permite que surjan ataques cibernéticos, filtraciones de datos sensibles y pérdidas económicas considerables.

En este entorno remoto, los empleados utilizan dispositivos personales y redes Wi-Fi no seguras, lo que incrementa el riesgo de amenazas tanto externas como internas, en este sentido, la escasa capacitación y la falta de conciencia sobre prácticas seguras entre los empleados han contribuido a que se conviertan en el eslabón más débil en la cadena de defensa cibernética. (Quirumbay et al., 2021)

En el contexto postpandemia, las empresas del municipio de Manaure, se han enfrentado a una oportunidad valiosa para reevaluar y fortalecer sus estrategias de ciberseguridad, ya que esta nueva realidad ha llevado a la empresa a adoptar un entorno de trabajo híbrido, lo que hace fundamental desarrollar un enfoque integral que no solo aborde las vulnerabilidades actuales, sino que también anticipe los riesgos futuros.

No obstante, se han enfrentado a desafíos significativos en este proceso, en donde es posible destacar, la falta de políticas de ciberseguridad claras y estructuradas, junto con la escasez de recursos y personal especializado en esta área, limita la capacidad de la empresa para implementar estrategias efectivas que protejan su infraestructura y datos; por lo que es necesario que se superen estos obstáculos para garantizar un entorno de trabajo seguro y confiable.

Al abordar esta problemática es fundamental para proteger la información y los datos de las empresas, así como para crear un ambiente laboral más seguro y confiable para los empleados que trabajan de forma remota.

En este contexto, una estrategia sólida de ciberseguridad no solo permitirá la continuidad operativa, sino que también generará confianza entre clientes y socios comerciales en su capacidad para enfrentar los desafíos del teletrabajo, por lo que este enfoque integral responde de manera efectiva a las amenazas cibernéticas y asegurar un futuro más seguro en sus operaciones.

Pregunta problematizadora

Finalmente, la pregunta central que motiva esta investigación es: ¿Cuáles son las estrategias de ciberseguridad más efectivas que pueden implementar las empresas del municipio de Manaure en el departamento de la Guajira, para asegurar un teletrabajo óptimo, seguro y eficiente?

Justificación

La presente investigación se justifica en la necesidad urgente de abordar el problema de ciberseguridad en el contexto del teletrabajo, especialmente en las empresas del municipio de Manaure en el departamento de la Guajira, al norte del territorio colombiano.

La adopción del teletrabajo, impulsada por la pandemia de COVID-19, ha transformado las dinámicas laborales, creando un entorno que expone a las organizaciones a diversas vulnerabilidades cibernéticas. (Tapasco y Giraldo, 2020) En la actualidad, la ciberseguridad se ha convertido en un componente crítico de la infraestructura empresarial moderna (Diaz y Rangel, 2020).

Según el Informe de Ciberseguridad 2023 de IBM, el costo promedio de una violación de datos a nivel mundial alcanzó los 4.45 millones de dólares (IBM, 2023), este incremento resalta la importancia de adoptar estrategias efectivas para proteger la información y la infraestructura empresarial, pues, a medida que más empresas optan por el teletrabajo, la protección de datos y la integridad de la información se vuelven esenciales (López y Sisa, 2020)

Por su parte, de acuerdo con un informe de Check Point Research (2022), señaló que los ataques cibernéticos a nivel global aumentaron en un 38% en comparación con 2021, con un promedio de 1,500 millones de intentos de ataques reportados semanalmente en todo el mundo.

En Colombia, la situación no es menos alarmante, ya que de acuerdo con un informe de la Cámara Colombiana de Comercio Electrónico (2022) reveló que el 67% de

las empresas colombianas ha experimentado al menos un incidente de seguridad cibernética en el último año, lo que evidencia la vulnerabilidad del entorno empresarial en el país.

Paralelamente, otro estudio demostró que el 75% de las organizaciones en Colombia considera que sus sistemas de ciberseguridad son insuficientes para afrontar los nuevos retos del teletrabajo (Cámara Colombiana de Comercio Electrónico, 2023), lo cual destaca la necesidad de fortalecer las políticas de ciberseguridad a nivel nacional para asegurar la continuidad de las operaciones empresariales en un contexto cada vez más digital.

En la Guajira, las brechas tecnológicas y la falta de inversión en infraestructura digital agravan la problemática, ya que según el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) reportó en 2021 que solo el 45% de las empresas en la región cuenta con políticas de ciberseguridad implementadas, lo que las hace altamente vulnerables a ciberataques (MinTIC, 2021).

De todo lo mencionado, las empresas del municipio de Manaure, no han estado excepta, ya que, la implementación del teletrabajo ha revelado la falta de una estrategia de ciberseguridad sólida (Talataa, s.f), lo cual ha provocado incidentes menores, pero con el potencial de escalar si no se implementan las medidas correctivas adecuadas. De esta manera, es esencial que estas empresas fortalezcan sus políticas de ciberseguridad para garantizar la protección de sus datos sensibles, la continuidad operativa y la confianza de sus clientes y socios comerciales.

Finalmente, esta monografía tiene el potencial de influir en la formulación de políticas, ya que sus hallazgos pueden servir como base para recomendaciones que

fortalezcan aspectos relevantes de ciberseguridad, promoviendo un enfoque más integral que beneficie a diversas industrias.

Objetivos

Objetivo general

Revisar las estrategias de ciberseguridad que sirven para la optimización del teletrabajo en las empresas del municipio de Manaure en el departamento de la Guajira.

Objetivos específicos

Identificar las principales vulnerabilidades de ciberseguridad asociadas al teletrabajo, considerando tanto las amenazas internas como externas que afectan a las empresas del municipio de Manaure en el departamento de la Guajira.

Analizar las políticas y estrategias de ciberseguridad propuestas en estudios y marcos regulatorios a nivel global y de Colombia, evaluando su aplicabilidad para el establecimiento de lineamientos que fortalezcan la seguridad digital en entornos de trabajo remoto.

Proponer recomendaciones que permitan la mitigación de riesgos asociados al teletrabajo, en las empresas del municipio de Manaure en el departamento de la Guajira, con el fin de mejora en la eficiencia operativa y la confianza de sus colaboradores y socios comerciales.

Estado del arte

Para elaboración de esta monografía fue necesaria la búsqueda de investigaciones previas que hablaran de la misma temática en donde en primera instancia, es importante mencionar el estudio realizado por Navarro (2020), el cual tuvo como objetivo elaborar una guía práctica de ciber seguridad, la cual estuvo dirigida a pequeñas y medianas, empresas enfatizando en la participación activa de los empleados en la protección digital.

Ésta se realizó a través de una revisión bibliográfica amplia en donde se identificó que la mayoría de los recursos existentes son altamente técnicos y poco accesibles para empresarios y trabajos, sin información especializada; dando como resultado el desarrollo de una guía clara y funcional, orientada a la realidad operativa de las pymes, por lo que, el aporte y la pertinencia de este estudio a la investigación monográfica en mure, ofrece herramientas adaptables que fortalece la seguridad desde una perspectiva colaborativa.

Seguidamente, es importante mencionar el estudio de Valero, el cual analizó el impacto de la ciberseguridad en las PYMES ecuatorianas tras la pandemia de COVID-19, con el objetivo de identificar el grado de implementación de mecanismos de seguridad informática. En este contexto, este estudio usó una metodología de carácter cualitativo, basado en una revisión bibliográfica y encuesta a representantes de las pequeñas empresas.

En donde los resultados reflejaron una deficiencia técnica y administrativa que incrementó la exposición a riesgos cibernéticos, concluyendo que una propuesta de buenas prácticas alineada a la norma ISO 27001, y COBIT 5.0. Por lo que este enfoque valioso para el estudio en cuestión, porque también se busca fortalecer la ciberseguridad digital después de la pandemia de COVID-19.

Por otra parte, el trabajo de Sánchez (2024), tuvo como objetivo desarrollar una guía de recomendaciones para la gestión de la ciber seguridad en el contexto del teletrabajo en pymes colombianas a través de una metodología descriptiva, en donde se analizó el concepto, clave y las normativas vigentes y los riesgos asociados al trabajo remoto.

Los resultados de este estudio evidenciaron la necesidad de estructurales políticas de seguridad de la información para prevenir amenazas y vulnerabilidades, por lo que la propuesta buscó facilitar la toma de decisiones y proteger los activos digitales de las empresas, aportando significativamente a este estudio, una base práctica para fortalecer la ciberseguridad en entornos laborales remotos.

Finalmente, el estudio realizado por Góchez et al. (2024), el cual tuvo como objetivo analizar las medidas de ciberseguridad aplicada a entornos de teletrabajo en empresas privadas en El Salvador mediante una metodología cualitativa basada en entrevistas y análisis documental.

Este estudio identificó prácticas y vulnerabilidades comunes, mostrando como resultados que muchas organizaciones carecen de protocolo sólidos de protección, lo que incrementa su exposición a amenazas, cibernéticas concluyendo que es urgente fortalecer la seguridad digital en el entorno del trabajo remoto, mediante prácticas integrales y de capacitación continua. Por lo que este estudio es relevante para el análisis de las estrategias aplicables en el teletrabajo en Manaure para que adopten enfoques exitosos dentro del contexto, laboral.

Marco teórico

Teletrabajo en la actualidad

De acuerdo con Roncal (2021), la pandemia del COVID 19 ha tenido impactos desastrosos en las estadísticas de empleo lo que ha conllevado a una crisis que tiene repercusiones adversas en el mercado laboral en especial se pueden señalar tres aspectos:

- ✓ El primero de estos es el incremento del desempleo y el subempleo a nivel mundial llegando a tener una escala de desempleo que va desde 5.3 millones a 24.7 millones considerando 180 millones de desempleados en el año 2019.
- ✓ El segundo aspecto se relación con un elevado incremento de los niveles de producción y despido de los trabajadores.
- ✓ El tercer aspecto se refiere a la afectación del 80% de la fuerza de trabajo debido a la ralentización de las actividades económicas lo que ha llevado a que los trabajadores se encuentren sin empleo o con salarios por debajo de 3,20 dólares diarios.

Para Padilla (1999) citado en Roncal (2021), el teletrabajo consiste en desarrollar una actividad laboral en un espacio diferente al asignado por la empresa o institución empleadora cliente para la que se trabaja; en él se realiza un empleo intensivo de las tecnologías de la información; y supone que el valor añadido que aporta el teletrabajador a la empresa está relacionado con el uso de esas tecnologías.

La pandemia de COVID-19 ha acelerado la adopción del teletrabajo en muchas empresas, transformando la forma en que se lleva a cabo la actividad laboral en diversas industrias. Este cambio abrupto hacia un entorno de trabajo remoto ha generado nuevos

desafíos en términos de ciberseguridad (Santillán, 2020); a medida que los empleados utilizan dispositivos personales y redes domésticas para realizar sus tareas, las organizaciones se enfrentan a un aumento significativo en las vulnerabilidades cibernéticas que pueden ser explotadas por atacantes.

De la misma manera Ramos et al (2020), mencionó que las brechas de seguridad se han ampliado, facilitando el acceso no autorizado a información confidencial y crítica, por lo que, es esencial que las empresas comprendan las amenazas que enfrentan al implementar esta modalidad, pues, la identificación y mitigación de estos riesgos no solo son cruciales para la protección de datos sensibles, sino que también son fundamentales para mantener la confianza de clientes y socios comerciales en un entorno laboral cada vez más digitalizado.

En este sentido organismo como el Instituto nacional de estándares y tecnología y la norma ISO 27,001 recomiendan el uso de controles técnicos concretos para ambientes de trabajo remoto, por lo que en estos destacan y la autenticación multifactorial, el cifrado de extremo a extremo, el control de acceso basado en privilegios y el uso de redes privadas virtuales, y también la gestión de parches de seguridad en los dispositivos remotos.

Además, es necesario reconocer que estas recomendaciones ideales enfrentan barreras particulares en el contexto de las pymes colombianas, específicamente en regiones como Manaure, ya que estas empresas, muchas veces con presupuestos limitados y bajo nivel de digitalización, no siempre cuentan con el personal capacitado ni políticas internas, claras.

Lo cual puede generar un desfase entre las recomendaciones internacionales y la realidad operativa, por lo que un diagnóstico aplicado en empresas de pequeña escala, hay evidenciado que las prácticas mínimas como copias de seguridad políticas de Contraseñas o robusta, segmentación de redes, son inexistentes.

Desde una perspectiva teórica, también es pertinente, introducir una discusión crítica sobre la postura de autores, aunque Roncal (2021) y Santillán (2020), resaltan el valor del teletrabajo como una respuesta funcional a las crisis. Otros estudios destacan las resistencias culturales y organizacionales frente a la implementación.

Un ejemplo es que algunos países presentan reticencia a adoptar marcos formales de ciber seguridad por desconocimiento, desconfianza o percepción de costo, por lo que esta atención entre lo ideal y lo factible debe analizarse con profundidad para diseñar soluciones que respondan verdaderamente al entorno de Manaure.

Finalmente, el teletrabajo no es una modalidad emergente que ha definido el empleo, sino que exige nuevas competencias de seguridad informática, y estas estrategias deben construirse desde una mirada técnica, contextual y crítica, que no sólo considera estándares globales, sino también la capacidad de adaptación de las pymes locales, ya que el reto está en traducir, las buenas prácticas internacionales, en acciones realistas y sostenibles para proteger el activo más valiosa de cualquier organización: la información

Ventajas del teletrabajo

De acuerdo con Osio (2010), la idea central del teletrabajo es que tenga un sentido de continuidad y actualización y confidencialidad para los trabajadores y la empresa de tal forma que entre las ventajas fundamentales se tiene:

- ✓ Flexibilidad para tener la decisión de cómo, dónde y cuándo trabajar.
- ✓ Tener la autonomía en la organización y desarrollo de las actividades.
- ✓ Posibilidad de realizar movilidades.
- ✓ Mayor productividad que se asocia a la libertad de realizar actividades y tener posición de decisión.
- ✓ Mayores oportunidades laborales
- ✓ Mejor calidad de vida familiar
- ✓ Oportunidades laborales para personas con discapacidad.
- ✓ Menor desplazamiento, menos molestias y estrés
- ✓ Capacidad de decidir el horario de trabajo y las pautas de trabajo.
- ✓ Creación de nuevas empresas y oportunidades para otros teletrabajadores.

Legalidad del teletrabajo en Colombia

Gracias a la pandemia según Molina (2022), es necesario repensar la ley 1221 de 2008 por ejemplo con el fin de flexibilizar el teletrabajo y ampliar el uso ahondando en estudios que permitan la evaluación del impacto que tiene la poca movilización que los trabajadores deben realizar hasta su sitio de trabajo contribuyendo con la huella de carbono.

Garantizar a los teletrabajadores derechos y garantías a distancia dado que la pandemia deja mucho que pensar en materia del trabajador por fuera de la empresa dado que no existe aún una manera estandarizada de monitorear a los trabajadores y sus distintas acciones.

Ciberseguridad y teletrabajo

De acuerdo con Camargo (2020), es un estándar para las empresas y personas ver en la informática una herramienta fundamental para su trabajo diario por lo que se hace indispensable acogerse a medidas que permitan la seguridad de la información y por lo tanto buscar las herramientas existentes que permiten a los teletrabajadores mantenerse lejos de posibles ataques cibernéticos que puedan atentar contra su integridad y la de la empresa en donde trabajan.

Por tal razón, es necesario tener muy en cuenta las fuentes jurídicas y el documento conpes 3854 de comercio electrónico, internacional y decretos 131 de 2020 que se firmó el 31 de mayo de 2020 y por eso se hace necesario que los trabajadores realicen procesos de actualización continuos en temas que se relacionan con la ciberseguridad debido a que para muchas personas en la actualidad esto se ha convertido en un mito difícil de creer y que tal vez no piensan pueda ocurrirles en determinado momento.

Vulnerabilidades de ciberseguridad en el teletrabajo

Las vulnerabilidades en el teletrabajo se dividen en amenazas internas y externas, cada una de las cuales representa riesgos significativos para las organizaciones. Las amenazas externas incluyen ataques de phishing, ransomware y malware, que han aumentado drásticamente en el contexto actual.

Según un informe de Cybersecurity Ventures (2023), se estima que los ataques cibernéticos han crecido un 400% desde el inicio de la pandemia, destacando la necesidad de adoptar medidas de seguridad robustas, por lo que, estos ataques pueden resultar en la pérdida de datos críticos, daños a la reputación y costos financieros considerables.

Por otro lado, las amenazas internas también son críticas. La falta de capacitación adecuada de los empleados en prácticas de ciberseguridad y el uso de dispositivos personales para acceder a la red corporativa convierten a los empleados en un eslabón débil en la defensa cibernética.

Un estudio de Verizon (2023) indica que el 30% de las brechas de seguridad son causadas por errores humanos, lo que subraya la importancia de la formación continua y de políticas claras en el uso de tecnología, por lo tanto, abordar ambas categorías de vulnerabilidades es esencial para garantizar un entorno de trabajo remoto seguro y eficiente.

Análisis de políticas y estrategias de ciberseguridad

A nivel global, existen marcos y políticas de ciberseguridad que pueden ser aplicables a las empresas colombianas, las cuales buscan establecer directrices efectivas para la protección de la información.

Un ejemplo destacado es el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST), que ofrece un enfoque integral para la gestión de riesgos cibernéticos, pues, este marco se basa en cinco funciones clave: identificar, proteger, detectar, responder y recuperar, lo que permite a las organizaciones desarrollar una estrategia robusta adaptada a sus necesidades específicas.

En Colombia, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) ha desarrollado normativas específicas para fortalecer la ciberseguridad en las empresas, ya que, estas regulaciones buscan establecer un marco claro que fomente la

implementación de políticas efectivas de seguridad cibernética y la capacitación de personal.

No obstante, la implementación de estas normativas es limitada en varias regiones, donde la falta de recursos y la escasa infraestructura digital dificultan su aplicación (MinTIC, 2021); por lo tanto, es fundamental que en las empresas de Colombia se consideren estos marcos y políticas para fortalecer su ciberseguridad y adaptarlas a su contexto operativo, mejorando así su capacidad de respuesta ante incidentes cibernéticos.

La ley 2121 de 2021, crea y regula la movilidad del trabajo remoto en Colombia, entendida como una relación laboral 100% virtual desde su inicio hasta su finalización sin que exista la presencia de ninguna de las fases del vínculo laboral, esta ley establece tanto para el empleador como para el trabajador, los medios tecnológicos, garantías laborales, derechos a la desconexión digital, y el respeto por las jornadas. (Congreso de Colombia, 2021)

Esta ley es fundamental para estructural, modelos de ciber seguridad que obliga a las empresas a garantizar medios tecnológicos adecuados, lo que incluye equipos y condiciones de seguridad de conexión al almacenamiento y transmisión de datos, por lo que su incorporación al estudio permite alinear las estrategias de seguridad con un marco jurídico que respalda la virtualidad total y permanente.

El Decreto 1227 de 2022, reglamenta en el artículo 17 de la ley 2088 del 2021, y establece los lineamientos operativos del trabajo en casa, con una modalidad ocasional o temprana, la cual permite al trabajador, desempeñar sus funciones fuera del lugar habitual de trabajo sin cambiar la naturaleza del vínculo laboral, por lo que define criterios sobre

tiempo, condiciones, reversibilidad y asignación de herramientas por parte del empleador. (Ministerio del trabajo, 2022)

Es importante mencionar que este decreto permite cubrir escenarios en los que los trabajadores no están en el trabajo permanente, pero si es necesarios por motivos como emergencias sanitarias, movilidad o necesidad organizativa, ya que su valor reside en el reconocimiento de la transitoriedad del trabajo remoto, lo cual exige a las pymes que cuenten con protocolos de ciber seguridad, dinámica y adaptable, es decir, incluso en casos de teletrabajo temporal, debe existir mecanismos de control, formación y mitigación de riesgos digitales.

Marco conceptual

Amenazas internas: Se refiere a riesgos que provienen del interior de la organización, generalmente por empleados o colaboradores por lo que estas amenazas pueden ser intencionales o accidentales, y afectan la seguridad al comprometer información sensible o interrumpir las operaciones normales de la empresa. (Alvariño, 2021)

Amenazas externas

Son acciones maliciosas realizadas por individuos o entidades externas a la organización con el fin de acceder, dañar o interrumpir sus sistemas y datos, por lo que, estas amenazas pueden tomar la forma de ataques de malware, phishing, o intentos de violación de seguridad en redes. (Alvariño, 2021)

Estrategias de ciberseguridad

Son planes y acciones implementados para proteger los sistemas informáticos y datos de una organización contra ciberamenazas, pues, estas estrategias incluyen la prevención, detección y respuesta a incidentes de seguridad, y se adaptan a las necesidades específicas de cada organización. (Urbanovics & Guajardo, 2022)

Políticas de ciberseguridad

Son directrices establecidas por una organización para garantizar la protección de su información y sistemas frente a amenazas cibernéticas, de acuerdo con Fonfría & Duch (2020), definen el uso adecuado de los recursos tecnológicos, las responsabilidades de los empleados y los procedimientos a seguir en caso de un incidente.

Evaluación de riesgos

Es el proceso mediante el cual se identifican, analizan y priorizan los riesgos potenciales que podrían afectar los sistemas de una organización, por lo que, la evaluación de riesgos permite a las empresas implementar medidas de control y mitigación para prevenir o reducir el impacto de posibles amenazas. (Obando et al., 2022)

Metodología

Método

Esta monografía empleó un método de revisión sistemática de literatura, la cual es una técnica estructurada que permite la recolección, clasificación, evaluación e interpretación de manera rigurosa y objetiva de estudios que ya existen acerca de un fenómeno determinado. (Pardal & Peláez, 2020)

Este método es diferente a la revisión narrativa, de acuerdo con Arias (2025), puesto que emplea un protocolo definido que la transparencia y replicabilidad del proceso de búsqueda y análisis de un proceso de búsqueda y análisis, en este caso, esta revisión se encuentra centrada en estudios que aborden las estrategias de ciber seguridad en el contexto de teletrabajo, particularmente en los escenarios similares al municipio de Manaure, o dentro del municipio de Manaure.

Esta metodología es especialmente adecuada, cuando se busca la generación de conocimiento consolidado a partir de diferentes fuentes, pues permite la identificación de patrones comunes, vacíos, investigativos, tendencias emergentes y prácticas exitosas que se adapten a la realidad local; asimismo, posibilita la evaluación, validez y aplicabilidad de estos modelos y políticas digitales, documentadas en diferentes contextos.

Paradigma

Esta monografía se enmarca en el paradigma interpretativo, puesto que parte de que, la realidad social es constituida por sujetos y debe ser comprendida a partir de los contextos específicos (de Franco & Solorzano, 2020).

Este enfoque es pertinente para el análisis de fenómenos complejos, como la ciberseguridad en entornos laborales, remotos, ya que no se limita sólo a cuantificar variables, sino que más bien busca comprender los certificados prácticos y precisiones en escenarios particulares.

Bajo este paradigma, se consideró que los desafíos del teletrabajo y la gestión de ciber seguridad informática, no pueden analizarse únicamente de una lógica técnica y normativa, pues es necesario incorporar dimensiones humanas, organizacionales y culturales que influyen en la adopción, eficacia y sostenibilidad de las estrategias implementadas; en este sentido, el paradigma interpretativo permitió el abordaje de la problemática desde una mirada holística, reconociendo la diversidad de factores que inciden en la construcción de entornos digitales, seguros.

Fuentes de información

Las fuentes de información que sustentan esta revisión fueron fundamentalmente secundarias y especializadas, lo cual implicó la consulta de literatura previa publicada y validar ámbitos académicos, técnicos institucionales.

En ello se incluyeron artículos científicos, indexados, tesis de grado y posgrado, libros especializados, documentos técnicos de organizaciones internacionales, normativas nacionales; del mismo modo, informes de consultoras reconocidas, lo cual permitió la garantía de la calidad y pertinencia del material revisado y favoreciendo un análisis profundo, contextualizado sobre las estrategias de ciber seguridad aplicables en el teletrabajo.

Bases de datos y repositorio

La recolección de información se realizó mediante una búsqueda en bases de datos científica de alto impacto, como lo son: Scopus, Scielo, Redalyc, IEEE Xplore, ProQuest y Google Scholar, que ofrecieron una literatura académica, multidisciplinar y actualizada. De la misma manera, se recurrió a repositorios institucionales de universidades reconocidas, tanto colombianas como extranjeras, que contaron con producción relevante en materia de ciberseguridad, transformación, digital o te teletrabajo.

De igual manera se incluyeron fuentes oficiales y sectoriales como informes técnicos de la cámara de comercio electrónico, el ministerio TIC, consultoría privadas, cuyos estudios ofrecieron datos cuantitativos, análisis, prospectivos y diagnóstico, sobre el estado actual de la ciberseguridad digital en el ámbito corporativo.

Criterios

Criterios de inclusión

- ✓ Publicaciones realizadas entre los años 2015 y 2025.
- ✓ Documentos redactados en español o inglés, que sean accesibles desde bases de datos académicas o repositorios oficiales.
- ✓ Estudios centrados en la relación entre ciberseguridad y teletrabajo, con interés en países en desarrollo o regiones con características socioeconómicas similares a La Guajira.
- ✓ Investigaciones con enfoque práctico, analítico o normativo.

Criterios de exclusión

- ✓ Publicaciones sin revisión por pares o cuya autoría no sea verificable.

- ✓ Documentos incompletos o sin acceso total al texto completo.
- ✓ Fuentes desactualizadas, fuera del rango temporal definido o desvinculadas del eje temático.

Proceso de búsqueda y selección

El proceso de búsqueda y selección se desarrolló de forma sistémica y progresiva, siguiendo una secuencia lógica que garantizó la relevancia del material recopilado, este estuvo conformado por diversas etapas, las cuales fueron:

Etapa uno: Se realizó una definición de las palabras claves y descriptores, teniendo en cuenta sinónimos variables lingüísticas y terminología técnica, perteneciente al objeto de estudio.

Fase dos: Se establecieron filtros de búsqueda, incluyendo rangos de tiempo entre 2015 y 2025; idioma español o inglés y tipo de publicación, documentos, académicos y técnicos revisados por pares.

Fase tres: Consistió en la aplicación de parámetros en la base de datos seleccionadas, seguido de una revisión inicial de títulos y resúmenes.

Fase cuatro: se procedió a la lectura del contenido completo de los textos pre seleccionados para la verificación de su calidad, metodológica, profundidad, analítica y pertinencia temática en relación con el contexto de ciberseguridad en entornos de teletrabajo.

Estrategias de búsqueda

Las estrategias de búsqueda, combinaron, términos, claves, estructurados mediante operaciones boléanos, los cuales permitieron el establecimiento de conexiones entre los conceptos fundamentales del estudio, adaptándose, según los estándares de cada base de datos, considerando su sintaxis y sistemas de indexación estos incluyeron:

$$"Ciberseguridad"\ AND\ "teletrabajo"\ AND\ ("Colombia"\ OR\ "empresas")$$

$$"Remote\ work"\ AND\ "cybersecurity"\ AND\ "strategies"$$

$$\text{Seguridad informática} AND \text{ trabajo remoto} AND \text{ entornos digitales}$$

Selección de estudios

El proceso de selección de estudios se organizó en dos fases sucesivas, en donde la primera consistió en una revisión exploratoria de los títulos y resúmenes con el objetivo de eliminar documentos que, a pesar de contener términos seleccionados, no respondían al objeto de estudio o carecían de un enfoque práctico o regional.

La segunda fase, por su parte, consistió en la preselección y sometimiento a lecturas, analíticas completas, considerando elementos como la solidez de su diseño metodológico, la claridad de los hallazgos y la aplicabilidad en contexto de empresariales comparables; los cuales incluyeron aquellos documentos que cumplían con todos los criterios de claridad, pertinencia y actualidad, previamente definida.

Análisis de datos

La información que se recopiló fue sometida a un proceso de codificación temática, a través del cual se identificaron y clasificaron las categorías emergentes más relevantes dentro del corpus documental.

Estas categorías incluyeron entre otras: tipos de amenazas cibernéticas, estrategias de mitigación implementadas, marcos regulatorios existentes, nivel de alfabetización digital, herramientas de protección utilizadas, y limitaciones operativas, observadas.

De modo que este análisis permitió la organización del conocimiento de manera coherente tanto con patrones comunes como elementos distintivos en cada uno de los textos estudiados, siendo la sistematización temática, quien facilitó la elaboración de conclusiones, comparativamente y contextualizadas

Extracción de la información

Para garantizar un tratamiento riguroso de datos, se diseñó una matriz de destrucción de información que recogió de forma estructurada de los elementos claves de cada fuente. Esta incluyó campos como nombre del autor o entidad de emisora, año de publicación, tipo de documento, objetivo del estudio, principal, hallazgo y finalmente aporte al estudio, lo cual facilitó el cruce de datos entre estudios, permitiendo la detención de convergencias, contracciones o vacíos relevantes en el corpus documental

Validación y fiabilidad

Con el fin de asegurar la validez interna y externa de análisis, se aplicó una triangulación metodológica, la cual consistió en el contraste de información proveniente de

fuentes diferentes enfoques Y niveles de análisis, permitiendo la verificación de la consistencia de los hallazgos y la reducción de riesgos de interpretación.

Paralelamente, se contó con el apoyo de expertos consultados en calidad de informantes, clave, entre ellos docentes, investigadores o profesionales del área de ciberseguridad, quienes validaron hallazgos preliminares y ofrecieron observaciones complementarias para el fortalecimiento de la credibilidad del estudio

Validación de las fuentes

En esta monografía, sólo se hizo uso de fuentes académicas, técnicas o institucionales que cuentan con un reconocimiento y respaldo verificable, por lo que se descartaron aquellas publicaciones que no estaban firmadas, que presentaban conflictos de interés evidente o que provinieron de sitios no acreditados.

Se prestó especial, atención en la reputación de los autores y organismos emisores, al número de citas o impacto académico del documento y la coherencia interna de su contenido. Para la garantía de la información utilizada, se tuvo en cuenta un alto nivel de fiabilidad y aplicabilidad.

Limitaciones del estudio

Entre las principales limitaciones se tuvo la escasez de estudios empíricos, específicamente centrados en el municipio de Manaure, lo cual exigió recurrir a fuentes análogas provenientes de contextos con condiciones socioeconómicas similares.

De la misma manera, la velocidad del cambio tecnológico en materia de ciberseguridad representa un reto para la vigencia de los hallazgos, ya que ciertas herramientas o amenazas pueden evolucionar rápidamente.

Finalmente, al tratarse de una investigación documental, no fue posible, recoger evidencia directa de prácticas, informales o situaciones no registradas en la literatura, lo que restringió la comprensión de ciertos matices locales.

Elaboración de conclusiones y recomendaciones

Las conclusiones derivaron de una síntesis crítica de los hallazgos categorizado, contrastando los con los objetivos de la investigación, permitiendo la identificación de estrategias efectivas y aspectos en la gestión de ciberseguridad en teletrabajo.

Para ello se formularon recomendaciones concretas, viables y adaptadas al contexto organizacional, tecnológico del municipio de Manaure, y se orientaron al fortalecimiento de capacidades institucionales, la mejora de la cultura digital y el establecimiento de políticas de protección sostenible.

Síntesis de hallazgos

Los resultados obtenidos fueron agrupados de manera temática en función de categorías previamente definidas, buscando resaltar las buenas prácticas identificadas, los factores críticos de éxito, las debilidades estructurales, persistentes y las normativas más eficaces.

Por lo que la intención de esta consolidación de hallazgos sirvió como una base empírica y conceptual para la toma de decisiones y el diseño de estrategias replicable en el ámbito local

Identificación de áreas futuras de investigación

Se proponen líneas de investigación futuras, que amplían y contemplan un enfoque del presente estudio, entre estas se incluyen el impacto de la cultura organizacional en la adopción de políticas de ciber seguridad, la efectividad de programas de capacitación digital en zona rurales, el uso de tecnologías emergentes e inteligencia artificial, en la gestión de riesgos, cibernéticos y la evaluación longitudinal de políticas de seguridad digital en empresas de pequeña escala.

Éstas representan una oportunidad valiosa para el fortalecimiento del conocimiento y la acción de estrategias en un entorno empresarial, cada vez más digitalizado y expuesto amenazas complejas.

Resultados

Caracterización de los estudios

Esta caracterización se encarga de detallar cada uno de los 25 documentos que fueron empiladas a lo largo de los resultados de la monografía, por lo que es su objetivo principal es mostrar una visión clara y estructurada de las referencias utilizadas, destacando aspectos fundamentales. Esta caracterización permite analizar la identificación, el origen y la naturaleza de cada fuente evidenciando la diversidad de materiales consultados que incluyen estudios académicos, informes técnicos, normas internacionales, leyes y políticas nacionales, así como documentos, sectoriales y tesis doctorales.

Asimismo, se resalta la pertinencia de cada documento en relación con los tres capítulos de los resultados, los cuales son vulnerabilidades y riesgos asociados al teletrabajo, análisis de políticas y marco regulatorios en ciber seguridad y las propuestas de mitigación paralas empresas del municipio de Manaure en el departamento de La Guajira.

De este modo, que facilita la comprensión integral del respaldo teórico y empírico que sustenta el análisis crítico realizado, evidenciado un equilibrio entre fuentes internacionales, nacionales y locales, que enriquecen en el abordaje temático y constituyen la formulación de recomendaciones contextualizadas viables.

Tabla 1.

Caracterización de los estudios

Autor / Entidad	Año	Tipo de documento	Tema principal / Enfoque	Contexto geográfico	Aplicabilidad / Uso en la monografía	Fuente / Referencia APA

Bermúdez & Cano	2023	Estudio académico / Informe	Amenazas internas y ciberseguridad en teletrabajo	Local	Identificación de vulnerabilidades internas en teletrabajo local	Bermúdez & Cano (2023)
Ibáñez & Rodríguez	2021	Estudio académico	Riesgos del uso de dispositivos personales (BYOD)	Local	Análisis de vulnerabilidades por BYOD en teletrabajo	Ibáñez & Rodríguez (2021)
Uribe	2023	Informe / análisis	Gestión de accesos y protocolos de seguridad	Local	Evaluación de controles internos en teletrabajo	Uribe (2023)
Castillo & López	2022	Estudio académico	Almacenamiento inseguro de información	Local	Impacto del almacenamiento inseguro en teletrabajo	Castillo & López (2022)
International Telecommunication Union (UIT)	2021	Informe técnico	Global Cybersecurity Index; medición global de madurez en ciberseguridad	Internacional	Marco para evaluación global y comparación de políticas en ciberseguridad	International Telecommunication Union (2021)
Aguilar	2021	Artículo académico	Adaptación del GCI para teletrabajo y trabajo híbrido	Internacional	Adaptación de indicadores para protección en teletrabajo	Aguilar (2021)
ISO / IEC	2022	Norma técnica	ISO/IEC 27001:2022, sistema de gestión de seguridad	Internacional	Directrices para manejo seguro de datos en trabajo remoto	ISO/IEC (2022)
National Institute of Standards and Technology (NIST)	2023	Marco de referencia	Cybersecurity Framework (NIST) para gestión de riesgos	Internacional	Marco flexible para gestión integral de cibersegurida	National Institute of Standards and Technology (2023)

					d en teletrabajo	
Sysoseva & Martínez	2025*	Informe / política	Políticas OCDE para resiliencia digital y cooperación internacional	Internacional	Recomendaciones para gestión de incidentes y cooperación en entornos remotos	Sysoseva & Martínez (2025)
Ministerio TIC (Colombia)	2024	Documento oficial / Política	Estrategia Nacional de Seguridad Digital 2025-2027	Colombia	Estrategia nacional para fortalecer seguridad digital en entornos remotos	Ministerio TIC (2024)
Congreso de la República de Colombia	2009	Ley	Ley 1273 de 2009 sobre delitos informáticos	Colombia	Marco legal para tipificación y sanción de ciberdelitos	Congreso de la República de Colombia (2009)
Función Pública Colombia	2012	Ley / reglamento	Ley 1581 de 2012, protección de datos personales	Colombia	Regulación del tratamiento de datos personales en teletrabajo	Función Pública (2012)
Función Pública Colombia	2018	Decreto	Decreto 1008 de 2018, política de gobierno digital	Colombia	Marco para digitalización segura en el sector público y privado	Función Pública (2018)
Organization of American States	2001	Convenio internacional	Convenio de Budapest sobre ciberdelincuencia	Internacional	Cooperación para combate internacional del ciberdelito	Organization of American States (2001)
Ministerio TIC (Colombia)	2023	Informe / política	COLCERT, grupo de respuesta ante incidentes cibernéticos	Colombia	Coordinación y monitoreo de incidentes cibernéticos	Ministerio TIC (2023)

Colombia Fintech	2024	Informe sectorial	Políticas empresariales de seguridad para pymes	Colombia	Buenas prácticas para pymes en teletrabajo	Colombia Fintech (2024)
Corredor	2021	Informe técnico	Protocolo de seguridad informática en empresa local	Local	Recomendación para protocolos de ciberseguridad	Corredor (2021)
Vanegas	2021	Estudio académico	Indicadores de productividad en teletrabajo	Local	Propuesta de indicadores claros de productividad	Vanegas (2021)
Pinto	2023	Estudio académico	Formación en competencias digitales	Local	Capacitación continua en herramientas digitales	Pinto (2023)
López & Velásquez	2023	Estudio sectorial	Comunicación interna en empresas locales	Local	Políticas de comunicación estructuradas	López & Velásquez (2023)
Sánchez et al.	2022	Estudio / informe	Protocolos VPN y seguridad en teletrabajo	Colombia	Implementación de VPN para proteger conexiones remotas	Sánchez et al., (2022)
Fuentes	2024	Estudio doctoral	Competencias digitales y gestión de tareas	Colombia	Capacitación para mejor desempeño en teletrabajo	Fuentes (2024)
Pérez	2022	Estudio académico	Canales de comunicación y gestión en teletrabajo	Colombia	Horarios y canales definidos para mejorar comunicación	Pérez (2022)
Rojas	2025	Tesis doctoral	Bienestar y ergonomía en teletrabajo	Colombia	Planes de bienestar para reducir estrés y fatiga	Rojas (2025)

Lechuga et al.	2021	Informe	Auditorías periódicas en teletrabajo	Colombia	Auditorías para asegurar cumplimiento normativo	Lechuga et al. (2021)

Nota: La tabla caracteriza los documentos y fuentes utilizadas para fundamentar el análisis, evaluación y propuestas sobre ciberseguridad y teletrabajo en el municipio de Manaure, destacando su origen, tipo, enfoque y relevancia para cada capítulo. *Fuente:* autoría propia.

Principales vulnerabilidades de ciberseguridad asociadas al teletrabajo en las empresas del municipio de Manaure (La Guajira)

El municipio de Manaure, ubicado en el departamento de la Guajira, se caracteriza por ser una zona con una economía predominante mente basada en la explotación salinera, el comercio local, la pesca artesanal y un creciente sector de servicios vinculados al turismo comunitario, pero la opción de herramientas digitales y esquemas de teletrabajo ha sido es igual ya que se ha encontrado influenciado por factores como la limitada, infraestructura tecnológica la intermitencia en el suministro eléctrico y la conectividad a Internet de las estabilidades, especialmente en zona rurales y comunidades indígenas.

A nivel de alfabetización digital, es importante mencionar que persiste una brecha significativa, de modo que un alto porcentaje de los trabajadores y micro empresarios mencionan que carecen de formación formal en el uso seguro de tecnologías de la información, lo que incrementa su exposición a riesgos cibernéticos, por lo que, en este contexto las empresas locales que han adoptado el teletrabajo, principalmente en el área administrativas, atención al cliente y comercio electrónico.

El presente capítulo examina las vulnerabilidades más relevantes vinculadas al teletrabajo, organizadas según su origen (interno o externo) y considera elementos

estructurales del entorno empresarial local que inciden directamente en la exposición a riesgos cibernéticos.

Amenazas internas

Las amenazas internas provienen de actores o procesos que operan dentro de la organización, en su mayoría no maliciosos, pero altamente riesgosos por desconocimiento o falta de control.

Tabla 2.

Amenazas internas

Vulnerabilidad	**Descripción**	**Impacto potencial**	**Autor**
Bajo nivel de conciencia sobre ciberseguridad	Escasa formación en buenas prácticas digitales.	Accesos no autorizados, pérdida de datos.	Bermúdez & Cano (2023)
Uso de dispositivos personales (BYOD)	Empleo de equipos no corporativos sin estándares de seguridad.	Contaminación cruzada, filtración de datos.	Ibáñez & Rodríguez (2021)
Gestión deficiente de accesos y privilegios	Permisos excesivos, falta de controles o monitoreo de usuarios.	Manipulación de información, fuga interna.	Uribe (2023)
Ausencia de protocolos de seguridad	Falta de políticas claras sobre protección de datos, contraseñas y redes.	Desorganización, exposición innecesaria.	Uribe (2023)
Almacenamiento inseguro de información	Uso de dispositivos USB o carpetas compartidas sin cifrado ni control de accesos.	Robo o pérdida de información crítica.	Castillo & López (2022)

Nota: La tabla identifica amenazas internas comunes en empresas de Manaure, describiendo su origen, efectos potenciales y autores que las documentan. *Fuente:* Autoría propia.

La tabla 1 muestra que la mayoría de las amenazas internas se encuentran relacionados con los factores humanos y procedimentales más que con los ataques deliberados, puesto que la falta de conciencia sobre irse, vivir seguridad es el eje central que agrava la tema vulnerabilidades, ya que, sin una cultura de protección digital, los empleados pueden sin intención, facilitar accesos, indebidos o pérdidas de datos.

El uso de dispositivo personales se presenta como un factor frecuente, especialmente en entornos de recursos limitados en donde la empresa no cuenta con los equipos corporativos; por lo que esta práctica aumenta de las posibilidades de contaminación cruzada y la fuga de información, dado que estos dispositivos externos suelen encarecer de antivirus, actualizados y cifrado de datos. Asimismo, la gestión es deficiente de acceso y la secuencia de protocolo claros indican un control interno, lo que no sólo eleva la exposición frente a incidentes, sino que dificulta la trazabilidad y respuesta ante eventos de seguridad.

Finalmente, el almacenamiento seguro mediante dispositivos USB, sin cifrado o carpetas compartidas abiertas, refleja la falta de política formal de gestión de datos sensibles en el contexto de Manaure, de modo que estas prácticas y potencializan la baja alfabetización digital y la escasez de recursos tecnológicos, lo que refuerza la urgencia de implementar capacitaciones periódicas, control estricto de acceso y directrices, claras para manejo de información.

Amenazas externas

En el contexto del teletrabajo en las empresas del municipio de Manaure se identificaron diversas amenazas externas que comprometen la integralidad disponibilidad y con fidelidad en la información corporativa. Esto proviene en gran medida de actores maliciosos, fuera de la organización que buscan explotar debilidades, tecnológicas humanas y procedimentales para obtener beneficios ilícitos o causar daño operativo.

Uno de los orígenes más comunes de estas amenazas, son ciberdelincuentes organizados a nivel internacional, quienes ejecutan campañas de phishing, malware y ransonware, dirigidas a empleados que trabajan desde sus hogares. También se identificaron riesgos procedentes de grupos de hackers oportunistas que operan en redes públicas, no seguras, como las ofrecidas en café o espacios comunitarios, interpretados en datos técnicos, particularmente en zona rurales donde la conectividad segura y limitada, obliga a los trabajadores a buscar alternativas de acceso en internet no protegidos.

Asimismo, existen amenazas derivadas de proveedores externos, comerciales, comprometidos, cuyos sistemas de seguridad no cumplen con los estándares adecuados.

Tabla 3.

Amenazas externas

Vulnerabilidad externa	**Descripción cualitativa**	**Impacto potencial**
Phishing dirigido (spear phishing)	Correos fraudulentos altamente personalizados que suplantan proveedores o entidades oficiales, aprovechando la confianza previa con la empresa.	Filtración de credenciales, acceso no autorizado a plataformas críticas.

Ataques de ransomware	Software malicioso que cifra la información corporativa accediendo desde conexiones remotas no seguras.	Pérdida de acceso a datos estratégicos, interrupción prolongada de operaciones.
Intercepción de datos en redes públicas	Robo de información transmitida por trabajadores que usan redes wi-fi abiertas en cafés o lugares públicos.	Exposición de datos confidenciales de clientes y procesos internos.
Suplantación de identidad digital	Creación de perfiles falsos en redes sociales o plataformas de trabajo para engañar a empleados y clientes.	Daño reputacional y fraude económico.
Explotación de vulnerabilidades en software desactualizado	Ataques que aprovechan fallas no corregidas en sistemas operativos y aplicaciones utilizadas para teletrabajo.	Control remoto de equipos, robo de información sensible.

Nota: La tabla describe amenazas externas comunes en el teletrabajo, sus características y el impacto potencial en empresas de Manaure. *Fuente:* autoría propia.

La tabla 2, evidencia que las vulnerabilidades externas más relevantes para las empresas en el municipio de Manaure, se concentran en ataques altamente personalizados de oportunistas, como lo son el phishing dirigido y suplantación de identidad digital, aprovechando la confianza y desconocimiento de algunos trabajadores, mientras que el ransomware y la intercepción de datos, se ven favorecidos por el uso de redes, pocos seguros y dispositivos y Sin protección robusta.

Asimismo, el uso del software desactualizado incrementa las derechas de seguridad, sobre todo en contexto donde los recursos tecnológicos son limitados y las actualizaciones dependen de conexiones de Internet, inestables, por lo que estas condiciones y hacen que la

seguridad perimetral tradicional se insuficiente requiriendo estrategias, adaptada al contexto local, que integra capacitación, actualización tecnológica y protocolo de verificación.

Análisis de políticas y estrategias de ciberseguridad globales y colombianas para fortalecer la seguridad digital en el trabajo remoto.

Este capítulo revisa las principales políticas y marcos regulatorios de ciberseguridad, tanto a nivel internacional como a nivel de Colombia, con el propósito de evaluar su aplicabilidad y así establecer lineamiento de efectivos en entornos de trabajo remoto, especialmente y contextos como el de Manaure en el departamento de la Guajira.

Marco y estrategias globales de ciber seguridad

En el ámbito internacional, la unión internacional de telecomunicaciones (UIT) y la organización para la cooperación del desarrollo económico (OCDE), promueve políticas orientadas a la resiliencia digital y el fortalecimiento de las capacidades técnicas y la cooperación internacional, (Ordenes et al., 2021) un ejemplo destacado es la global, cibersecurity index (GCI), la cual establece las dimensiones clave como el Marco legal, medidas técnicas, desarrollo de capacidades y cooperación, fortaleciendo indicadores que pueden adaptarse para entornos de teletrabajo y trabajo híbrido. (Aguilar, 2021)

La ISO/IEC 27001:2022, una norma ampliamente reconocida, probé directrices para establecer un sistema de gestión de seguridad de información con controles aplicables a la gestión remota de datos y mecanismos para minimizar riesgos asociados al acceso fuera de las instalaciones, por su parte, el Cybersecurity Framework [NIST] (2023), enfatiza cinco funciones esenciales, las cuales son identificar, proteger, detectar, responder y recuperar que ofrecen una estructura flexible para organizaciones de cualquier tamaño sector,

permitiendo su personalización escenarios de movilidad laboral y conexión remota. Estos marcos coinciden en la necesidad de implementar políticas específicas para trabajo remotos, priorizando en la autenticación multifactor, el cifrado de extremo a extremo, la segmentación de redes, la gestión de parches de seguridad y la capacitación constante de higiene digital.

Tabla 4.

Marco y estrategias globales de ciber seguridad

Marco / Estrategia	**Organismo emisor**	**Enfoque principal**	**Aplicaciones clave para teletrabajo**	**Fortalezas relevantes**	**Fuente**
Global Cybersecurity Index (2021)	UIT	Medición de preparación y madurez en ciberseguridad	Evaluar el nivel de protección de un país/organización; orientar políticas de teletrabajo seguro	Visión global y comparativa; fomenta cooperación internacional	International Telecommunication Union, (2021)
ISO/IEC 27001:2022	ISO / IEC	Gestión integral de la seguridad de la información	Controles para acceso remoto, manejo de datos sensibles, continuidad de negocio	Certificación internacional; adaptable a cualquier sector	ISO/IEC, (2022)
NIST Cybersecurity Framework (2023)	National Institute of Standards and	Marco flexible de gestión de riesgos	Implementar ciclo continuo de identificación, protección,	Guías detalladas; adaptable a organizacion	National Institute of Standards and Technology, (2023)

	Technology (EE. UU.)		detección, respuesta y recuperación	es de todos los tamaños	
Políticas OCDE de resiliencia digital	OCDE	Cooperación internacional y desarrollo de capacidades	Recomendaciones para gestión de incidentes en trabajo remoto, intercambio de información	Énfasis en cooperación y estándares globales	Sysoseva & Martínez (2025)

Nota: La tabla presenta políticas y estrategias clave de ciberseguridad globales y colombianas, destacando objetivos, enfoques y aplicaciones relevantes. *Fuente:* (ISO, 2022)

Estrategias y políticas de ciberseguridad en Colombia

Colombia está consolidando un ecosistema de ciberseguridad, robusto a través de un conjunto de estrategias políticas y marcos regulatorios que integran aspectos técnicos, legales, institucionales y sociales, en primera instancia el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) lidera la Estrategia Nacional de Seguridad Digital 2025-2027, cuyo objetivo central es el fortalecimiento de la resiliencia del país, frente a los ciber ataques, dando garantía de un entorno digital, seguro para ciudadanos, empresas o instituciones públicas.

Esta estrategia se apoya en un marco legal consolidado que incluye la ley 1273 del 2009, qué tipifica los dedico informáticos y protege la información de los datos, de la misma manera, la ley 1581 de 2012, la cual regula la protección de los datos personales, y el decreto 1008 de 2018, que establece la política de gobierno digital, haciendo promoción, el uso confiable y competitivo de las TIC.

Asimismo, en Colombia, también se ha fortalecido su cooperación internacional, participando activamente en redes como Interpol y Europol y ratificando el convenio con Budapest sobre ciber delincuencia, de modo que a nivel operativo se consolida la CONCERT, que es un grupo de respuestas de emergencias, cibernéticos, la cual se encarga de coordinar y responder ante incidentes de seguridad digital. Además, se han desarrollado centros regionales de ciber seguridad como el que se proyecta en Caldas, que también funcionará como un centro de formación ciudadana y se promueve la inversión privada en infraestructura de ciberseguridad con actores, como CLARO implementando medidas avanzadas para proteger a los usuarios

Tabla 5.

Estrategias y políticas de ciberseguridad en Colombia

Estrategia / Norma	**Objetivo principal**	**Medidas clave**	**Aplicabilidad en entornos de teletrabajo y zonas rurales**	**Fuente**
Estrategia Nacional de Seguridad Digital 2025-2027	Fortalecer la resiliencia ante ciberataques y proteger el bienestar digital	Gestión integral de riesgos, cooperación público-privada, protección de derechos digitales	Planes de respuesta adaptados a conectividad limitada y protocolos de contingencia offline	Ministerio TIC, (2024)
Ley 1273 de 2009	Tipificar delitos informáticos y sancionar suplantación, acceso no	Marco penal para perseguir cibercrimen	Refuerza la disuasión de ataques internos y externos en teletrabajo	Congreso de la República de Colombia, (2009)

	autorizado, daño a datos			
Ley 1581 de 2012	Proteger datos personales y regular su tratamiento	Políticas de privacidad, consentimiento informado, registros	Aplicable en manejo de datos de clientes y empleados en entornos remotos	Función pública (2012)
Decreto 1008 de 2018 (Gobierno Digital)	Promover el uso seguro y confiable de las TIC	Digitalización segura de procesos y servicios	Favorece la gestión digital corporativa segura en zonas apartadas	Función pública (2018)
Convenio de Budapest	Combatir el ciberdelito mediante cooperación internacional	Intercambio de información y asistencia legal transfronteriza	Permite rastrear amenazas que afectan a teletrabajadores desde el exterior	Organization of American States. (2001)
COLCERT	Coordinar la respuesta ante incidentes cibernéticos	Monitoreo, alerta temprana, atención a incidentes	Asesoría remota a empresas sin personal especializado en ciberseguridad	Ministerio TIC. (2023)
Centros regionales de ciberseguridad	Capacitación y respuesta local ante incidentes	Formación ciudadana, infraestructura de monitoreo	Ideal para reforzar capacidades en municipios apartados	Ministerio TIC (2024)
Políticas empresariales de seguridad	Establecer controles internos y formación continua	Capacitación, análisis de riesgos, protocolos de seguridad	Aumenta la resiliencia de pymes con recursos limitados	Adaptado de Colombia Fintech. (2024)

Nota: La tabla describe y relaciona políticas y estrategias nacionales de ciberseguridad con su aplicabilidad en teletrabajo y zonas de Colombia. *Fuente:* autoría propia.

Evaluación de aplicabilidad de políticas y marcos de ciberseguridad para teletrabajo

La evaluación de la aplicabilidad de las políticas y marcos de ciber seguridad y entornos de teletrabajo, se llevó a cabo mediante un análisis comparativo de referentes internacionales y nacionales, orientados la identificación de buenas prácticas, estándares y regulaciones que puedan adaptarse al contexto colombiano, específicamente en el municipio de Manaure. Para ello, se revisaron los documentos normativos anteriormente, identificados como guías, técnicas y estudios académico, provenientes de organizaciones como la hizo la unión internacional de telecomunicaciones así los marcos regulatorio establecidos en Colombia por el ministerio de las TIC la ley 1581 del 2011, entre otros

El proceso de evaluación se fundamenta en tres criterios principales, primero la pertinencia que es el grado en que la medida y los lineamientos se ajustan a las características técnicas ilegales y culturales del teletrabajo en Colombia; Seguidamente, la viabilidad, que es la factibilidad de implementación de los lineamientos, considerando recursos humanos, tecnológicos y financieros disponibles en las organizaciones; finalmente, en la escala habilidad que es la posibilidad de qué las medidas pueden ser aplicadas en organizaciones de diferentes tamaños y sectores.

Para sistematizar la evaluación se elaboró una matriz que permitió comparar los elementos claves de cada política o marco de referencia, identificando aquellos que ofrecen un valor agregado significativo para la protección de la información y la continuidad operativa en entornos laborales remotos.

Tabla 6.

Evaluación de aplicabilidad de políticas y marcos en entornos de teletrabajo.

Marco o política	Enfoque principal	Fortalezas para teletrabajo	Limitaciones identificadas	Nivel de aplicabilidad en Colombia
ISO/IEC 27001	Gestión de seguridad de la información	Estructura clara para implementar un SGC; adaptable a teletrabajo; enfoque en riesgos.	Requiere inversión y personal capacitado.	Alta (para medianas y grandes empresas).
NIST SP 800-46 Rev. 2	Seguridad en teletrabajo y acceso remoto	Guías prácticas sobre VPN, autenticación multifactor y gestión de dispositivos.	Basado en entorno normativo de EE. UU., requiere adaptación legal.	Media-Alta (tras contextualización).
UIT – Directrices de ciberseguridad para pymes	Buenas prácticas de ciberseguridad	Lenguaje accesible, adaptable a empresas pequeñas.	Menor profundidad técnica para entornos complejos.	Alta (especialmente en micro y pequeñas empresas).
Ley 1581 de 2012 (Colombia)	Protección de datos personales	Marco legal obligatorio; protege derechos de titulares.	No aborda medidas técnicas específicas para teletrabajo.	Alta (aplicable en todo el territorio).
MinTIC – Guía de teletrabajo seguro	Seguridad digital en trabajo remoto	Contextualización al entorno colombiano; recomendaciones prácticas.	Alcance limitado en temas de ciberinteligencia y respuesta a incidentes.	Muy alta (alineada al contexto nacional).

Nota: La tabla sintetiza la valoración de marcos y políticas internacionales y nacionales para fortalecer la seguridad digital en teletrabajo. *Fuente:* autoría propia.

En términos generales, se puede decir que la evaluación reveló que la combinación de estándares internacionales con políticas y guías nacionales, ofrece una base sólida para establecer línea mientras de seguridad digital aplicable al teletrabajo en Colombia en el entorno del municipio de Manaure, sin embargo se identificó la necesidad de fortalecimiento en la capacitación del talento humano y en la inversión de infraestructura tecnológica, en cuanto a la adopción de mecanismos de monitoreo continuo para garantizar la eficiencia en las medidas.

Recomendaciones que permitan la mitigación de riesgos asociados al teletrabajo

El teletrabajo como modalidad clave para garantizar la continuidad operativa de las empresas, brinda reducción de costos y amplia la flexibilidad laboral, de modo que ha traído consigo riesgos, que de no gestionarse adecuadamente, pueden afectar la eficiencia como la confianza interna y externa de las organizaciones entre otros riesgos se encuentra: la disminución del control de las actividades, el problema de la ciberseguridad del aislamiento laboral, la disminución del compromiso organizacional y las fallas de la comunicación.

En este sentido, el municipio de Manaure en donde las empresas operan en entornos cambiantes y con recursos limitados, es fundamental proponer recomendaciones que permitan la mitigación de estos riesgos, de tal manera que estas medidas respondan a la realidad local, aprovechando las herramientas tecnológicas disponibles, fomentando, la cultura organizacional, sólida y asegurando la protección de los datos y la integralidad de los procesos.

Por tal razón, en este punto se presentan las recomendaciones prácticas, su relación con la mitigación del riesgo y la forma en que impactar las empresas del municipio, tanto en la mejora de la eficiencia, como en la consolidación de la confianza de los colaboradores y socios comerciantes.

Tabla 7.

Recomendaciones para mitigar riesgos del teletrabajo en empresas de Manaure

Recomendación propuesta	**Mitigación de riesgo asociado**	**Aplicación en empresas de Manaure**			**Fuente**
		Mejora de la eficiencia	**Confianza de colaboradores**	**Confianza de socios comerciales**	
Implementar protocolos de ciberseguridad	Reduce riesgos de robo de información y ataques informáticos	Minimiza interrupciones por incidentes cibernéticos.	Garantiza seguridad en el manejo de datos personales.	Asegura la protección de información estratégica compartida.	Corredor (2021)
Establecer indicadores claros de productividad	Evita la disminución del rendimiento por falta de control de tareas	Permite seguimiento objetivo del desempeño.	Brinda claridad en expectativas y metas.	Demuestra capacidad de cumplir compromisos con calidad y tiempos establecidos.	Vanegas (2021)
Capacitación continua en herramientas digitales	Reduce errores operativos y dependencia excesiva de soporte técnico	Aumenta autonomía y destreza tecnológica.	Genera seguridad en el manejo de software y plataformas.	Refuerza la imagen de empresa moderna y preparada.	Pinto (2023)

Políticas de comunicación interna estructuradas	Disminuye el riesgo de desinformación y malentendidos	Evita retrasos por falta de información.	Fomenta transparencia y cohesión de equipo.	Garantiza fluidez en el intercambio de información clave.	López & Velásquez (2023)
Implementar protocolos de uso de VPN	Pérdida o filtración de información	Reducción de tiempos muertos por ataques informáticos	Seguridad percibida por los empleados al manejar datos	Mayor seguridad en transacciones y manejo de información sensible	Sánchez et al., (2022)
Capacitación en competencias digitales y gestión de tareas	Baja productividad por desconocimiento de herramientas	Incremento en la velocidad y calidad de ejecución de tareas	Mayor autonomía y motivación	Cumplimiento oportuno de compromisos	Fuentes (2024)
Establecer horarios y canales de comunicación definidos	Descoordinación y duplicidad de esfuerzos	Flujo de trabajo más ordenado	Disminución del estrés y claridad de roles	Información consistente y confiable	Pérez (2022)
Crear un plan de bienestar y ergonomía para teletrabajadores	Fatiga, estrés y problemas de salud ocupacional	Reducción de ausentismo	Mejor clima laboral y compromiso	Estabilidad operativa que respalda la relación comercial	Rojas (2025)
Realizar auditorías periódicas de teletrabajo	Riesgo de incumplimiento normativo o contractual	Ajustes rápidos ante fallos	Transparencia en la evaluación del desempeño	Imagen positiva frente a aliados estratégicos	Lechuga et al. (2021)

Nota: Esta tabla se elaboró a partir del análisis de lineamientos de teletrabajo del Ministerio de Trabajo de Colombia (2022), estudios sobre gestión remota en entornos empresariales y buenas prácticas de ciberseguridad para pymes. *Fuente:* autoría propia.

La recomendaciones propuestas apuntan a tres ejes centrales, los cuales son: eficiencia, operativa, confianza interna y credibilidad externa, en materia deficiencia en las acciones más relevantes son la implementación de protocolos tecnológicos y capacitación digital, lo que asegura que los recursos sean utilizados de forma óptima, en cuanto a la confianza con los colaboradores, establecer canales de comunicación claros y planes de bienestar, que contribuyen a la reducción de incertidumbre y fortalecimiento del sentido de pertinencia. Finalmente, la confianza de los socios comerciales se afianza con prácticas transparencia cumplimiento y seguridad en el manejo de la información, garantizando así las relaciones sostenibles a largo plazo

Conclusiones

En primera instancia, es importante concluir que, la vulnerabilidad de la ciberseguridad refleja un panorama preocupante en donde la limitada infraestructura tecnológica, y la baja a la alfabetización digital, actúan como factores estructurales que agravan los riesgos; en cuanto a las amenazas internas, se evidencia una falla profunda en la cultura organizacional de seguridad con prácticas como el uso indiscriminado de dispositivos personales y ausencia de protocolos claros, lo que facilita brecha de seguridad evadidas. Paralelamente en las amenazas externas potentes y sofisticadas explotan las debilidades, sumando un desafío complejo en un contexto de conectividad inestable y recursos limitados, por lo que esta realidad demanda soluciones tecnológicas y también un cambio integral en capacitación y gestión, haciendo un ajuste en el contexto socioeconómico local.

Seguidamente, en cuanto a las política globales y nacionales, los resultados evidenciaron que existen marcos sólidos como la ISO/IEC 27001 y el NIST pero su implementación en contextos locales como Manaure, enfrenta barreras por limitaciones tecnológicas y de capital humano; si bien, las estrategias colombianas lideradas Ministerio de las TIC y el marco legal vigente aportan un contexto normativo adecuado, pero requiere mayor adaptación práctica para zona rurales con conectividad precaria. En este sentido, la sinergia entre estándares internacionales y políticas nacionales, es fundamental, aunque insuficiente si no se tiene un enfoque robusto en capacitación y monitoreo continuo.

De este modo, las recomendaciones propuestas para mirar los riesgos en el teletrabajo evidencian un enfoque integral que vincula, eficiencia, operativa, confianza, interna, credibilidad externa; sin embargo, su efectividad es dependiente de la superación

de barreras locales, como las limitaciones tecnológicas y la baja cultura digital, por lo que, la implementación de protocolos de ciber seguridad y la capacitación continua son esenciales para evitar vulnerabilidades técnicas, por lo que, requieren inversión y compromiso organizacional. De igual modo, fortalecer la comunicación y el bienestar laboral contribuye a la reducción del aislamiento y la mejora del compromiso del colaborador, por lo que estas medidas son necesarias, pero deben ir acompañadas de un soporte institucional y recursos adecuados para dar garantía a la sostenibilidad y adaptación del contexto del municipio de Manaure.

Finalmente, la revisión de estas estrategias de ciberseguridad aplicables al teletrabajo en las empresas de la Guajira, evidenció que la optimización de esta modalidad depende de la implementación de marcos políticos, adelantadas al contexto local. Por lo que, a pesar de las limitaciones tecnológicas y la brecha de alfabetización digital, la adopción de normas internacionales como ISO/IEC 27001, junto con las normas nacionales y protocolos específicos para el trabajo remoto, pueden fortalecer la protección de la información y la continuidad operativa; no obstante, para lograr los resultados efectivos es indispensable fomentar la capacitación constante, mejorar la infraestructura y promover la cultura organizacional, orientada a la seguridad digital

Recomendaciones

Se recomienda mejorar la tecnología disponible y ofrecer capacitación constante en seguridad digital a todos los empleados, puesto que esto ayuda a que las empresas reduzcan riesgos causados por falta de conocimiento y problemas técnicos adaptándose a la realidad local del municipio de Manaure.

Se recomienda adaptar las normas internacionales y nacionales de ciberseguridad a las condiciones específicas del municipio, especialmente para las pequeñas empresas y acompañar las conformación práctica y seguimiento regular para superar las limitaciones tecnológicas y de personal

Se recomienda a los futuros estudios profundizar en el análisis de cómo estas limitaciones tecnológicas y brechas de alfabetización digital, afectan a la implementación de políticas de ciber seguridad en contexto rurales como Manaure.

Finalmente, es importante dar paso a la investigación de estrategias innovadoras, adoptadas culturalmente, que faciliten la capacitación continua, la cultura organizacional en seguridad digital, así como evaluar el impacto de estas medidas en la sostenibilidad y efectividad del teletrabajo de pequeñas y medidas empresas locales.

Referencias bibliográficas

Aguilar, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. *Estudios internacionales (Santiago)*, *53*(198), 169-197. https://www.scielo.cl/scielo.php?pid=S0719-37692021000100169&sc

Alvariño, I. Á. O. (2021). La política exterior de los países del Golfo Pérsico: dinámicas internas y amenazas externas (introducción). *Revista española de ciencia política*, (56), 13-19. https://dialnet.unirioja.es/descarga/articulo/8024132.pdf

Arias, F. (2025). El artículo de revisión narrativa: nivel de evidencia y validez científica. Revisión semi-sistemática. *e-Ciencias de la Información*. https://revistas.ucr.ac.cr/index.php/eciencias/article/view/59584

Bermúdez, C., Cano M, J. J. (2023). *Modelo de Ciberseguridad para el Sector Logístico y Transporte Terrestre.* https://aisel.aisnet.org/isla2023/2/

Bueno, G. G. (2022). *Ciberseguridad post Covid-19 y su impacto en las pymes del Ecuador* [Tesis de maestría, Universidad Estatal Península de Santa Elena]. Repositorio UPSE. https://repositorio.upse.edu.ec/handle/46000/8979

Camacho, J. I. (2021). *El teletrabajo, la utilidad digital por el COVID 19.* https://www.redalyc.org/journal/4296/429671777006/html/

Cámara Colombiana de Comercio Electrónico. (2022). *Informe de seguridad cibernética en Colombia 2022. Cámara Colombiana de Comercio Electrónico.* https://www.ccce.org.co/informe-seguridad-cibernetica-2022

Cámara Colombiana de Comercio Electrónico. (2023). Estado de la ciberseguridad. MinTIC. https://www.mintic.gov.co/portal/implementacion-ciberseguridad

Camargo, L. (2020). Ciberseguridad y Teletrabajo. https://repository.urosario.edu.co/server/api/core/bitstreams/42006458-01cb-4fbb-a497-8f4f8f6302e9/content

Cano, W. D., Monsalve, S. (2023). *Ciberseguridad, reto empresarial para afrontar la era de la digitalización actual* (Bachelor's thesis, Escuela de Economía, Administración y Negocios). https://repository.upb.edu.co/handle/20.500.11912/11318

Check Point Research. (2022). 2022 Cyber Security Report. Check Point Software Technologies. https://www.checkpoint.com/cyber-security-report-2022

Colombia Fintech. (2024). Recomendaciones en ciberseguridad empresarial. https://colombiafintech.co/2025/07/22/asi-colombia-fortalece-su-estrategia-de-ciberseguridad-que-significa-esto-para-tu-empresa/

Congreso de Colombia. (2021). *Ley 2121 de 2021. Por medio de la cual se regula el trabajo remoto y se dictan otras disposiciones*. Diario Oficial No. 51.748, de agosto 3 de 2021. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=166184

Corredor, J. F. (2021). *Propuesta de mejoramiento del sistema de seguridad informática para el Instituto Cristo Rey, ubicado en la ciudad de Fonseca, La Guajira.* https://repository.libertadores.edu.co/items/27efb2f7-3bb6-4dc6-94e0-c47c28294102

Cybersecurity Ventures. (2023). Cybersecurity Market Report. Cybersecurity Ventures. Retrieved from https://cybersecurityventures.com

de Franco, M. F., Solórzano, J. L. V. (2020). Paradigmas, enfoques y métodos de investigación: análisis teórico. *Mundo recursivo*, *3*(1), 1-24. https://atlantic.edu.ec/ojs/index.php/mundor/article/view/38

Díaz, M. O., Rangel, P. E. S. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Revista criminalidad, 62(2), 199-217. https://revistacriminalidad.policia.gov.co:8000/index.php/revcriminalidad/article/download/168/258

Fonfría, A., & Duch, N. (2020). Elementos para una política de ciberseguridad efectiva. Análisis del Real Instituto Elcano (ARI), 127, 2020. https://media.realinstitutoelcano.org/wp-content/uploads/2021/10/ari127-fonfriaduchbrown-elementos-para-politica-de-ciberseguridad-efectiva.pdf

Fonfría, A., Duch, N. (2020). Elementos para una política de ciberseguridad efectiva. Análisis del Real Instituto Elcano (ARI), 127, 2020. https://media.realinstitutoelcano.org/wp-content/uploads/2021/10/ari127-fonfriaduchbrown-elementos-para-politica-de-ciberseguridad-efectiva.pdf

Fonfría, A., Duch, N. (2020). Elementos para una política de ciberseguridad efectiva. Análisis del Real Instituto Elcano (ARI), 127, 2020. https://media.realinstitutoelcano.org/wp-content/uploads/2021/10/ari127-fonfriaduchbrown-elementos-para-politica-de-ciberseguridad-efectiva.pdf

Fuentes, Y. R. (2024). *La Gamificación como Estrategia Didáctica para el Fortalecimiento de las Competencias Digitales de los Docentes en las Áreas Básicas de 2 grado del IET Rural Agropecuaria de Mingueo-La Guajira* (Doctoral dissertation, Universidad de Cartagena). https://repositorio.unicartagena.edu.co/server/api/core/bitstreams/cd440e25-bb67-4973-ae7b-b79098411851/content

Función pública. (2009). Ley 1273 de 2009. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Función pública. (2012). Decreto 1008 de 2018. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=86902

Función pública. (2012). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Góchez, J. P., Rivas, M. R., Solorzano, J. F. (2024). *Ciberseguridad aplicada en entornos de teletrabajo para empresas del sector privado en El Salvador* [Tesis de maestría no publicada]. Universidad Don Bosco. http://hdl.handle.net/11715/2775

Guaña, E. J., Sánchez, A., Chérrez, P., Chulde, L., Jaramillo, P. D. C., Pillajo, C. (2022). Ataques informáticos más comunes en el mundo digitalizado. https://dspace.itsjapon.edu.ec/jspui/handle/123456789/3445

Ibáñez, C. A., Rodríguez, L. F. (2021). *Construcción de guías de hardening que eleven los niveles de seguridad para los funcionarios de entidades financieras que laboran*

desde la modalidad del teletrabajo. https://repository.ucatolica.edu.co/handle/10983/25732

IBM. (2023). Cost of a Data Breach Report 2023. IBM Security. https://www.ibm.com/reports/data-breach

IBM. (2023). Cybersecurity and the Remote Workforce. IBM Security. Retrieved from https://www.ibm.com/security

Instituto Nacional de Estándares y Tecnología (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity (Versión 1.1). National Institute of Standards and Technology. https://www.nist.gov/cyberframework

International Telecommunication Union. (2021). *Global Cybersecurity Index 2020.* https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Cybersecurity-Index.aspx

ISO/IEC. (2022). *ISO/IEC 27001:2022 – Information Security Management Systems.* International Organization for Standardization. https://www.iso.org/standard/27001

Lazos, L. E. C., Ruiz, J. M. P., García, J. J. G. (2024). Análisis de Productividad en la Industria Manufacturera en México Antes y Durante la Pandemia del Covid-19. Ciencia Latina: Revista Multidisciplinar, 8(2), 5648-5663. https://dialnet.unirioja.es/servlet/articulo?codigo=9565957

Lechuga, A., Manga, J., Espitia, J., Hernández, J. (2021). Buenas prácticas de teletrabajo para los colaboradores del área de auditoría en salud en Barranquilla. https://bonga.unisimon.edu.co/items/c5bc6e4b-350a-4696-95ad-75ccd6f200b4

López, D. A. M., Sisa, F. G. P. (2020). Teletrabajo como estrategia de competitividad y desarrollo para las empresas en el Ecuador. Revista Eruditus, 1(2), 53-70. http://revista.uisrael.edu.ec/index.php/re/article/view/318

López, M. J. A., Velásquez, O. J. V. (2023). *Análisis de las Tendencias de las Empresas en el Municipio de Maicao–La Guajira en el Periodo de Tiempo 2018–2022*. https://repositorio.udes.edu.co/server/api/core/bitstreams/ab873391-dc3c-4670-a73f-5417d66ad3e0/content

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2021). Política Nacional de Ciberseguridad 2020-2025. Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. https://www.mintic.gov.co/

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). Estado de la ciberseguridad en Colombia. MinTIC. https://www.mintic.gov.co/portal/implementacion-ciberseguridad

Ministerio del Trabajo. (2022). Decreto 1227 de 2022. Por el cual se reglamenta el trabajo en casa y se dictan otras disposiciones. Diario Oficial No. 52.091, de julio 18 de 2022. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=124095

Ministerio TIC. (2023). Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT). https://www.colcert.gov.co

Ministerio TIC. (2024). Centros de Ciberseguridad Regionales. https://www.mintic.gov.co

Ministerio TIC. (2024). Estrategia Nacional de Seguridad Digital 2025-2027. https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/403023:La-Estrategia-Nacional-de-Seguridad-Digital-llega-para-enfrentar-las-crecientes-

amenazas-cibernetics#:~:text=El%20Gobierno%20Nacional%20present%C3%B3%20la,desarrollo%20integral%20de%20las%20personas.

Molina, C. y Roncancio, A. (2022). Teletrabajo y Trabajo en casa, tendencias contemporáneas de contratación laboral en Colombia. Recuperado de: https://www.redalyc.org/journal/825/82570824020/html/

National Institute of Standards and Technology. (2023). *NIST Cybersecurity Framework (CSF) Version 2.0*. U.S. Department of Commerce. Recuperado de https://www.nist.gov/cyberframework

Navarro, C. (2020). *Estrategias de ciberseguridad: el caso de la pequeña y mediana empresa* [Trabajo de fin de máster, Universidad de Zaragoza]. Facultad de Ciencias Sociales y del Trabajo. https://zaguan.unizar.es/record/101988/files/TAZ-TFG-2020-1242.pdf

Obando, C., Garcés, L. F., Quiroz, J., Benjumea, M., Valencia, A., Zavala, L. R., Patiño, C. (2022). Evaluación de riesgos en ciberseguridad: una revisión bibliométrica. Revista Ibérica de Sistemas e Tecnologias de Informação, (E49), 396-409. https://search.proquest.com/openview/30ab36bec36b2b520b869c1fbbe32eb6/1?pq-origsite=gscholar&cbl=1006393

Órdenes, X., Roberts, R., Rojas, P., Rojas, F. (2021). *Estrategia de transformación digital.* https://repositorio.cepal.org/bitstream/handle/11362/49067/1/S2300491_es.pdf

Organization of American States. (2001). Convenio sobre la ciberdelincuencia. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Osio Havriluk, L. (2010). El Teletrabajo: Una opción en la era digital Observatorio Laboral Revista Venezolana, vol. 3, núm. 5, enero-junio, 2010, pp. 93-109 Universidad de Carabobo Valencia, Venezuela. https://www.redalyc.org/pdf/2190/219014912006.pdf

Pardal, J. L., Pardal, B. (2020). Anotaciones para estructurar una revisión sistemática. *Revista orl*, *11*(2), 155-160. https://scielo.isciii.es/scielo.php?pid=S2444-79862020000200005&script=sci_arttext&tlng=en

Pérez, J. A. (2022). Establecer y analizar las redes sociales y medios virtuales como canales para el mejoramiento de la comunicación externa en la Secretaría de Educación Localidad de Kennedy. https://repository.universidadean.edu.co/entities/publication/46952752-8137-4536-82b5-7f228edb2f4b

Pinto, A. R. (2023). *Diseño e implementación de un modelo de formación para el desarrollo de la competencia digital docente en futuros maestros de la Universidad de la Guajira*. https://repositori.uib.es/xmlui/handle/11201/160480

Quirumbay, D. I., Castillo, C. A., Coronel, I. A. (2022). Una revisión del aprendizaje profundo aplicado a la ciberseguridad. Revista Científica y Tecnológica UPSE (RCTU), 9(1), 57-65. http://scielo.senescyt.gob.ec/scielo.php?pid=S1390-76972022000200057&script=sci_arttext

Ramos, V., Ramos, C., Tejera, E. (2020). Teletrabajo en tiempos de COVID-19. Revista Interamericana de Psicología/Interamerican Journal of Psychology, 54(3), e1450-e1450. https://www.journal.sipsych.org/index.php/IJP/article/view/1450

Rojas, K. I. F. (2025). *Estrategias y buenas prácticas en el marco del Sistema de Gestión de Seguridad y Salud en el Trabajo, para mejorar la salud mental de los empleados de una empresa de servicios que laboran bajo modalidad de home office en Colombia* (Doctoral dissertation, Fundación Universitaria del Área Andina). https://digitk.areandina.edu.co/bitstreams/37021c27-0d30-4ae9-b61d-e3a772dde5bb/download

Roncal Vattuone, Ximena. (2021). Teletrabajo y Capitalismo de Vigilancia. Telos: revista de Estudios Interdisciplinarios en Ciencias Sociales, 23 (1), Venezuela. (Pp. 177-192). https://www.redalyc.org/journal/993/99365404014/99365404014.pdf

Sánchez, A. F. (2024). *Gestión de la ciberseguridad en el teletrabajo para pymes en Colombia* [Monografía de grado, Universidad Nacional Abierta y a Distancia - UNAD]. Repositorio UNAD. https://repository.unad.edu.co/handle/10596/56540

Sánchez, C. R., Gavilán, M. C., Mateus, M. Á. (2022). *Buenas prácticas en seguridad de la información para el teletrabajo en Colombia*. https://repository.libertadores.edu.co/bitstreams/9a7eabb0-1c5f-499b-967c-96dd28005158/download

Santillan, W. (2020). El teletrabajo en el COVID-19. CienciAmérica: Revista de divulgación científica de la Universidad Tecnológica Indoamérica, 9(2), 65-76. https://dialnet.unirioja.es/servlet/articulo?codigo=7746439

Sysoseva, L., Martínez, M. J. (2025). De la seguridad a la gobernanza digital en OCDE: evolución y algunas consideraciones actuales desde la transformación digital. https://roderic.uv.es/items/b700fb94-36c0-4a2f-8d93-183ccb1b2076

Tapasco, O. A., Giraldo, J. A. (2020). Asociación entre posturas administrativas de directivos y su disposición hacia la adopción del teletrabajo. Información tecnológica, 31(1), 149-160. https://www.scielo.cl/scielo.php?pid=S0718-07642020000100149&script=sci_arttext

Torrealba, L. M. L. (2024). Transformación laboral en la era digital: Impacto de la IA en las relaciones laborales. *Revista sobre Relaciones Industriales y Laborales*, (56), 34-55. https://revistasenlinea.saber.ucab.edu.ve/index.php/rrii2/article/view/7163

Urbanovics, A., Guajardo, R. (2022). Estrategias de ciberseguridad en los países latinoamericanos–un análisis comparativo. Acta Hispanica, (IV), 89-104.

Uribe, D. (2023). *Gestión de vulnerabilidades de aplicación interna*. https://repositorio.tdea.edu.co/handle/tdea/3570

Vanegas, C. A. (2021). *Análisis de la capacidad de innovación de la Universidad de La Guajira: una propuesta de mejora*. https://bdigital.uexternado.edu.co/entities/publication/cc586117-d88f-4060-8061-dc5543ced8e4

Verizon. (2023). Data Breach Investigations Report. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

Appendices

Apéndice a.

Aplicabilidad y retos de políticas y estrategias nacionales para teletrabajo

	A	B	C	D	E	F
1	**Estrategia / Norma**	**Año**	**Enfoque**	**Beneficios para teletrabajo**	**Desafíos en zonas rurales y pymes**	**Fuente**
2	Estrategia Nacional Seguridad Digital	2025-27	Fortalecer resiliencia y protección digital	Adaptación a conectividad limitada; protocolos offline	Limitaciones tecnológicas y falta de formación	Ministerio TIC (2024)
3	Ley 1273 de 2009	2009	Tipificación de delitos informáticos	Marco legal penal que protege datos y usuarios	Difícil seguimiento en contextos rurales	Congreso Colombia (2009)
4	Ley 1581 de 2012	2012	Protección de datos personales	Obliga a cumplir estándares de privacidad	Aplicación desigual en pequeñas empresas	Función Pública (2012)
5	Decreto 1008 de 2018	2018	Promoción de gobierno digital	Digitalización segura y competitiva	Brecha tecnológica en municipios apartados	Función Pública (2018)
6	CONCERT (Grupo respuesta)	2023	Coordinación ante incidentes	Respuesta rápida y monitoreo de amenazas	Requiere mayor presencia y recursos locales	Ministerio TIC (2023)
7						

Apéndice b.

Evaluación estadística

Marco o política	Pertinencia (1-5)	Viabilidad (1-5)	Escalabilidad (1-5)	Comentarios relevantes
ISO/IEC 27001	4.5	3.0	4.0	Alta pertinencia, requiere inversión técnica y humana.
NIST SP 800-46 Rev. 2	4.0	2.8	3.8	Buena guía técnica, adaptación legal necesaria.
Directrices UIT para Pymes	3.8	4.2	4.5	Muy viable para pequeñas empresas, menor profundidad.
Ley 1581 de 2012 (Protección de datos)	4.7	4.0	4.3	Fuerte marco legal, poca orientación técnica.
Guía MinTIC para teletrabajo	4.3	4.1	4.2	Adaptada al contexto nacional, limitada en ciberinteligencia.

Interpretación:

La Ley 1581 obtiene la mayor puntuación en pertinencia por su marco legal obligatorio.
La Guía MinTIC y las Directrices UIT para Pymes destacan en viabilidad y escalabilidad, especialmente en contextos de recursos limitados.
El ISO/IEC 27001 es muy pertinente y escalable, pero su viabilidad se ve afectada por costos y necesidad de personal especializado.
El NIST es muy técnico y detallado, pero requiere ajustes legales y contextuales para su adopción en Colombia.